METHOD AND APPARATUS FOR IMPROVING EFFICIENCY OF END-USER CERTIFICATE VALIDATION

Abstract Of The Disclosure

An apparatus and method collects, for a community of interest, at least one cross certificate associated with an anchor certificate issuing unit, and obtains at least one certificate issuing unit public key and an associated unique identifier for a cross-certified certificate issuing unit identified by the at least one cross certificate. For example, a certificate issuing unit, client unit, or other suitable unit, searches for one or up to all certification authorities or certificate issuing units that it can trust based on cross certificate chains. This is done, for example, from a given trust anchor. The apparatus selects those obtained certificates that satisfy, for example, some search criteria, such as what policy must be enforced in each certificate, for example, the allowed path length or depth that the apparatus is allowed to evaluate, and creates a signed certificate set, such as a list of all trusted certificate issuing units from the perspective of a given trust anchor. Accordingly, the apparatus and method creates a signed certificate set identifying certificate issuing units determined to be trusted by the anchor certificate issuing unit based on the cross certificates that the apparatus obtained. The signed certificate set includes at least a unique identifier of each trusted certificate issuing unit , such as the distinguished name (DN) of the certificate issuing unit, and public key of each trusted certificate issuing unit.